National Infrastructure Protection Center
CyberNotes

Issue #2000-09 *May 10, 2000*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, hacker exploit scripts, hacker trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between April 20 and May 4, 2000. The table provides the hardware/operating system, equipment/software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates from previous issues of CyberNotes are listed in bold. New information contained in the update will appear as red and/or italic text.**

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Aladdin Knowledge Systems [1]	eToken 3.3.3x	A vulnerability exists which could allow a malicious user the ability to access all private information stored on the device without knowing the PIN number of the legitimate user.	No workaround or patch available at time of publishing.	Aladdin Knowledge Systems eToken PIN Extraction	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Apple[2] MacOS 9.0	AppleShare IP 6.1-6.3	A vulnerability exists in the http server, which could allow a remote malicious user to mine data from a site running this package.	Upgrade available at: http://asu.info.apple.com/swupdates.nsf/artnum/n11670 (If you are currently running either AppleShare IP 6.1, 6.2 or 6.3, first upgrade to Mac OS 9.0.4 and AppleShare IP 6.3.1 before you install AppleShare IP Web & File 6.3.2.)	AppleShare IP 6.x Invalid Range Request	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[1] L0pht Research Labs Security Advisory, May 4, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Atrium Software[3] Windows 95/98/NT 4.0	Cassandra NNTP Server 1.10	An unchecked buffer overflow vulnerability exists in the code that handles login information, which could cause the server to stop responding.	No workaround or patch available at time of publishing.	Cassandra Buffer Overflow	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Atrium Software[4] Windows 95/98/NT	Mercur Mailserver 3.2 and below	A security vulnerability exists in the IMAP server, which could allow a remote malicious user that has access to the IMAP server to access arbitrary files.	No workaround or patch available at time of publishing.	Mercur Mailserver Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Brecht Claerhout[5] Unix	Sniffit 0.3.7beta; Sniffit 0.3.6HIP;	A buffer overflow vulnerability exists which can exploited remotely by malicious users to gain root access.	No workaround or patch available at time of publishing.	Sniffit Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Cisco[6]	IOS 9.14, 12.0.1W-12.0.7, 12.0, 12.0(5)T, 12.0(9)S, 12.0DB, 12.0S, 12.0T, 11.2-11.2.9XA, 11.1.13, 11.1.15, 11.1.16, 11.1.17, 11.1	A vulnerability exists in the online help, which could allow security-related information to be retrieved by an unprivileged user logged on to a Cisco router.	Cisco's Product Security Incident Response Team recommends the following workaround. A security-conscious Cisco router configuration should perform the following actions: - Set the default privilege level for access lines to 0 (rather than leave at 1, the default) - Using "privilege exec," specify which commands a user at level 0 can use. This will severely restrict the options a non-enabled user will have, thereby implementing a "default deny" stance on the router itself.	Cisco Router Online Help	Medium/ **[**]**High**	Bug discussed in newsgroups and websites. Exploit has been published.

---

[2] Bugtraq, May 2, 2000.
[3] USSR Advisory Code, USSR-2000039, May 1, 2000.
[4] Securiteam, April 27, 2000.
[5] s0ftpr0ject Advisory, SPJ-003-000, May 2, 2000.
[6] Bugtraq, May 2, 2000.

[**] **High due to Phrack 55 discussion concerning Bastion routers and Phrack 56 discussion of rerouting techniques and a published tunneling script.**

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Cisco[7]	IOS 11.0, 11.2x, 11.3x, 12.0x	A Denial of Service vulnerability exists if remote administration via HTML interface is enabled.	No workaround or patch available at time of publishing. Temporary workaround: (Securiteam) Turn off management via HTTP with the following configuration: *no IP http server*	Cisco IOS HTTP Denial of Service	Low/ **High** **(High if DDoS best-practices not in place)**	Bug discussed in newsgroups and websites. Exploit has been published.
FileMaker, Inc.[8] Windows NT 4.0. MacOS 8.0, 8.1, 8.5, 8.6, 9.0	FileMaker Pro 5.0	Several security vulnerabilities exist in the Web Companion software database package, which could allow remote malicious users the ability to retrieve, via XML, any data from a web-connected database, regardless of the security settings. The e-mail feature also allows malicious web users to anonymously forge e-mails.	No workaround or patch available at time of publishing.	FileMaker Web Companion Software Multiple Vulnerabilities	Medium	Bug discussed in newsgroups and websites. Vulnerability has appeared in the Press.
FreeBSD[9] Unix	FreeBSD 3.4	A buffer overflow vulnerability exists in the port of ncurses (a high-level terminal manipulation library) which can be used by a malicious user to obtain root access.	No workaround or patch available at time of publishing.	FreeBSD ncurses Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Hewlett-Packard[10] Unix	HP-UX 10.20, 11.00	A vulnerability exists in the automountd routine, which could allow a malicious user to execute arbitrary commands with the privileges of root.	Patches available at: ftp://ftp/export/patches/hp-ux_patch_matrix	HP Automountd	**High**	Bug discussed in newsgroups and websites.
IBM[11]	AIX 4.3., 4.3.1, 4.3.2	A vulnerability exists in the frcactrl program, part of the Fast Response Cache Accelerator (FRCA) package, which could allow local malicious users to utilize this program to modify files. This could lead to a compromise of the root account on the machine.	Until an official fix is available, IBM recommends removing the setuid bit from the frcactrl command: # chmod 555 /usr/sbin/frcactrl	AIX frcactrl Insecure File Handling	**High**	Bug discussed in newsgroups and websites.

[7] Securiteam, Mar 2, 2000.
[8] SecurityFocus, May 2, 2000.
[9] Buffer 0verfl0w Security Advisory # 3, April 24, 2000.
[10] Daily Security Bulletins Digest, HPSBUX9910-104, May 3, 2000.
[11] ISS Security Advisory, April 26, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
ICRadius[12]	ICRADIUS 0.14	A buffer overflow vulnerability exists which could allow a remote malicious user to execute arbitrary commands on the server.	No workaround or patch available at time of publishing.	IC Radius Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Id Software Inc.[13] Windows 95/98/NT 4.0	Quake3 Arena 1.16n	A directory traversal vulnerability exists which could allow a malicious user to read or write files, install Trojan horse programs, or gather passwords on a computer that has the software installed. **This vulnerability is important to network administrators who may be unaware that users are accessing potentially malicious Quake3Arena servers outside their network.**	Id Software fixed the flaw in its latest patch release, Version 1.17, released on Wednesday. at: http://www.quake3arena.com/	id Software Quake3Arena Directory Traversal	Medium/ **High** **(High if network security best practices not in place.)**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the Press.
IMP[14]	IMP 2.0.11	Two security vulnerabilities exist: one could allow the exposure of sensitive document information, and the other can be used to cause a Denial of Service.	The first vulnerability has been fixed in the 2.2 beta version.	IMP 2 Vulnerabilities	Medium	Bug discussed in newsgroups and websites.
LBL[15]	Tcpdump 3.4-3.5	A vulnerability exists in the DNS decode capabilities which could result in an infinite loop. If tcpdump is being used as some part of and intrusion detection system, this could allow an remote malicious user the ability to evade this system.	No workaround or patch available at time of publishing.	Tcpdump DNS Decode	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
McMurtrey/ Whitaker & Associates, Inc.[16] Win32-based servers	Cart32 2.6, 3.0	A software backdoor exists which could allow remote malicious users the ability to run arbitrary commands on the serer and/or gain access to credit card information.	Patch available at: ftp://ftp.cart32.com/v30latestbuilds/c32admin.exe	Cart32 Remote Administration Password	**High**	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the Press.

[12] Securiteam, May 2, 2000.
[13] Internet Security Systems Security Advisory, May 3, 2000.
[14] Crimelabs Security Advisory, CLABS200003, April 24, 2000.
[15] Bugtraq, May 2, 2000.
[16] Cerberus Information Security Advisory, CISADV000427, April 27, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft[17] Windows 95/98	Windows 95/98	A vulnerability exists when a NetBIOS session packet is received with the source host name set to NULL, which could result in everything from lockups, reboots and "the blue screen of death" to total loss of network connectivity. This specifically targets the Messenger service on Windows 95/98.	No workaround or patch available at time of publishing.	Microsoft Windows 9x NetBIOS NULL Name	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Multiple Vendors[18] Unix	LCDProc 0.4	Multiple buffer overflow vulnerabilities exist which could allow a remote malicious user to execute arbitrary code.	Downgrading to a previous version of LCDProc, which does not utilize a client/server model, will eliminate this problem.	Multiple Vendor Linux LCDProc Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Multiple Vendors[19] Windows 95/98/NT 4.0, Unix	L-Soft Listserv 1.8	A buffer overflow vulnerability exists in the Web Archives component, which could allow remote malicious users can execute arbitrary code.	L-Soft has created an update to ListServ to address this issue. For more information e-mail support@lsoft.com	L-Soft Web Archives Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Multiple Vendors[20] Unix	Qualcomm qpopper 3.0, 2.53; RedHat imap 4.5-4; University of Washington imap 4.5	A number of pop3 daemon implementations contain numerous buffer overflows, which could allow a malicious user to execute arbitrary code.	No workaround or patch available at time of publishing.	Closed Mail Server	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Multiple Vendors[21, 22] Unix	RedHat Linux 6.1, 6.2; Mandrake 7.0	A symbolic link (symlink) vulnerability exists in OpenLDAP, which could allow a local malicious user the ability to destroy the contents of any file on any mounted filesystem.	Patch available at: RedHat: ftp://updates.redhat.com/6.1 Mandrake: Please upgrade to: e15137088145d315952586f1ad6330ef openldap-1.2.9-5mdk.i586.rpm 0807d4c34bf6cec47fede3cf7c2572c5 openldap-1.2.9-5mdk.src.rpm	RedHat Openldap Symlink Overwrite Denial	Medium	Bug discussed in newsgroups and websites.

[17] el8.org advisory, May 2, 2000.
[18] Securiteam, April 24, 2000.
[19] Cerberus Information Security Advisory, CISADV000503, May 3, 2000.
[20] Bugtraq, April 20, 2000.
[21] RedHat Security Advisory, RHSA-2000:012, April 24, 2000.
[22] Mandrake Security Update, April 22, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
NetBSD[23]	NetBSD 1.4.2 SPARC, Alpha; 1.4.1 SPARC, Alpha; 1.4 SPARC, Alpha	A Denial of Service vulnerability exists when a packet is remotely sent with an unaligned IP timestamp option.	No workaround or patch available at time of publishing.	NetBSD Unaligned IP Option Denial of Service	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Netwin[24] Windows 9/98/NT 4.0, Unix, MacOS 9.0	DMail 2.5d	A buffer overflow vulnerability exists which can be exploited remotely by a malicious user allowing execution of arbitrary code.	Patch available at: ftp://ftp.netwinsite.com/pub/dmailweb/beta/	Netwin Dmailweb Server utoken Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
ON Technology[25] Multiple Systems	Meeting Maker 1.0-6.0	Due to poor encryption of passwords while in transit, user credentials can be obtained by anyone sniffing the network.	ON Technology has released the following statement, including suggestions for mitigating the impact of this weakness: http://support.on.com/support/mmxp.nsf/31af51e08bcc93eb852565a90056138b/11af70407a16b165852568c50056a952?OpenDocument	Meeting Maker Weak Password Encryption	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
PostgreSQL[26] Unix	PostgreSQL 6.3.2, 6.5.3	A cleartext file storage vulnerability exists which could allow a user, with read access, the ability to obtain the password.	No workaround or patch available at time of publishing.	PostgreSQL Cleartext Passwords	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Qualcomm[27] Windows 95/98/NT 4.0	Eudora 4.2, 4.3	Eudora does not prompt a user with the warning message if they are attempting to open a file that is .exe, .com, or .bat.	No workaround or patch available at time of publishing.	Eudora 4.2/4.3 Warning Message Circumvention	**High**	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the Press.
RedHat[28] Unix	Linux 6.2 alpha, 6.2.i386, 6.2 sparc	A vulnerability exists in the passwd.php3 component which could allow malicious users to execute commands on the server. In conjunction with the backdoor password in Piranha, this could allow an anonymous remote malicious user to compromise the system.	Patches available from RedHat at: ftp://updates.redhat.com/6.2/	RedHat Piranha Virtual Server Package Passwd.php3 and Default Account and Password	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the Press.

[23] NHC 20000504a.0, May 4, 2000.
[24] Cerberus Information Security Advisory, CISADV000504, May 4, 2000.
[25] SecurityFocus, April 24, 2000.
[26] SecurityFocus, May 1, 2000.
[27] SecurityFocus, April 28, 2000.
[28] RedHat Inc. Security Advisory, RHSA-2000:014-10, April 24, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
RedHat[29] Unix	Linux kernel 2.1.x, 2.2.x, 2.3.x	A Denial of Service vulnerability exists in the knfsd daemon which could allow a remote unauthenticated user to render the NFS service inoperable.	Upgrade to the latest versions of the 2.2.x (2.2.15-pre20) or 2.2.3 (2.3.99-pre7) kernel will remedy this problem. Patch available at: ftp://ftp.kernel.org/pub/linux/kernel/people/alan/pre-patch-2.2.15-19to20.bz2	Linux knfsd Denial of Service	Low/ **High** **(High if DDoS best practices not in place.)**	Bug discussed in newsgroups and websites.
Sendmail Inc.[30]	Sendmail 8.9.x	Multiple unsafe fgets vulnerabilities exist which could allow a malicious user to insert LMTP commands into e-mail messages; create a possible deadlock between sendmail and mail.local; corrupt a user's mailbox; or change e-mail headers of the message in the user's mailbox.	No workaround or patch available at time of publishing.	Sendmail Multiple Unsafe Fgets()	Low/ Medium	Bug discussed in newsgroups and websites.
SourceGear Corporation[31]	Concurrent Versions System (CVS) 1.10.	A Denial of Service vulnerability exists due to predictable temporary filenames.	No workaround or patch available at time of publishing.	CVS Local Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Sun MicroSystems [32] Unix	Solaris 6.0, 7.0	A buffer overflow vulnerability exists in lpset, which could allow a local malicious user to gain root privileges.	Sun has released patches for Solaris 2.6 and 7: 107115-04 for Solaris 7 106235-05 for Solaris 6	Solaris Lpset Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Sun MicroSystems [33]	Solaris 7.0, 7.0_x86	A buffer overflow vulnerability exists in xsun, which could allow a local malicious user to execute arbitrary code and gain root privileges.	No workaround or patch available at time of publishing.	Solaris Xsun Buffer Overrun	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Sun MicroSystems [34]	Solaris 7.0, 7.0_x86	A buffer overflow vulnerability exists in the lp program, which could allow a malicious user to execute arbitrary code as root.	No workaround or patch available at time of publishing.	Solaris Lp -d Option Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[29] Bugtraq, May 1, 2000.
[30] Bugtraq, April 21, 2000.
[31] Bugtraq, April 23, 2000.
[32] Securiteam, April 26, 2000.
[33] Securiteam, April 27, 2000.
[34] Securiteam, May 2, 2000.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
SuSE[35] Unix	Linux 6.0-6.4	A vulnerability exists which could allow malicious users to delete any file in the root directory on the system.	Patches available at: S.u.S.E. Linux 6.4: ftp://ftp.suse.com/pub/suse/i386/update/6.4/a1/aaa_base-2000.4.27-1.i386.rpm S.u.S.E. Linux 6.3 alpha: ftp://ftp.suse.com/pub/suse/axp/update/6.3/a1/aaa_base-2000.1.3-0.alpha.rpm S.u.S.E. Linux 6.3: ftp://ftp.suse.com/pub/suse/i386/update/6.3/a1/aaa_base-2000.1.3-0.i386.rpm S.u.S.E. Linux 6.2: ftp://ftp.suse.com/pub/suse/i386/update/6.2/a1/aaa_base-99.9.8-0.i386.rpm	SuSE Linux Arbitrary File Deletion	Medium	Bug discussed in newsgroups and websites. Exploits have been published.
SuSE[36] Unix	S.u.S.E. Linux 6.3, 6.4	A vulnerability exists in the handling of the DISPLAY variable, which could allow a malicious user the ability to execute arbitrary code with the permissions of the user running the binary. This may be used to elevate privileges, and result in local root compromise.	No workaround or patch available at time of publishing.	S.u.S.E. Gnomelib Buffer Overflow	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Trend Micro[37] Windows NT 4.0	InterScan Virus Wall 3.0.1, 3.2.3, 3..3, 3.32	A vulnerability exists in the SMTP gateway, which could allow a remote malicious user to execute code with the privileges of the daemon. The code can be used to compromise the entire operating system.	A release of InterScan VirusWall 3.4 Beta can be found at: ftp://ftp.antivirus.com/products/beta/isvw34beta.zip	InterScan VirusWall uuencoded Remote Filename Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
UltraScripts[38] Windows, Unix	UltraBoard 1.6	A directory traversal vulnerability exists which could allow a remote malicious user the ability to open any file on the webserver (with its permissions).	No workaround or patch available at time of publishing.	UltraBoard Directory Traversal	Low	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Zone Labs[39] Windows 95 2.1, 98 2.1, NT 4.0.2.1	ZoneAlarm 2.1.10 & prior	A vulnerability exists which could allow malicious users to port scan the firewall without being detected.	Zone Labs is offering a Beta to correct this problem: http://www.zonelabs.com/beta_download.htm	ZoneAlarm Personal Firewall Port 67	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[35] SuSE Security Announcement, May 2, 2000.
[36] Securiteam, May 4, 2000.
[37] Network Associates, Inc. COVERT Labs Security Advisory, May 4, 2000.
[38] Bugtraq, May 3, 2000.
[39] SecurityFocus, April 24, 2000.

*Risk is defined in the following manner:

High - A vulnerability that will allow an intruder to immediately gain privileged access (e.g., sysadmin, and root) to the system. An example of this would be a vulnerability in which a sequence of instructions is sent to a machine by an unauthorized user and the machine responds with a command prompt.

Medium - A vulnerability that will allow an intruder immediate access to the system that is not privileged access. This allows the intruder the opportunity to continue the attempt to gain root access. An example would be a configuration error that allows an intruder to capture the password file.

Low - A vulnerability that provides information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. The reader should note that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered as a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between April 21 and May 4, 2000, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that hackers/crackers are utilizing**. During this period, 58 scripts, programs, and net-news messages containing holes or exploits were identified.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
May 4, 2000	**Heimlich.zip**	**Exploit script for the Aladdin Knowledge Systems eToken PIN Extraction vulnerability.**
May 3, 2000	Listservbo.c	Script which exploits the L-Soft web archives buffer overflow vulnerability.
May2-4, 2000	**Nmap-2.52.tgz**	**Added very simple man pages for xnmap/nmapfe. Also fixed a "Status: Down" machine name output problem in machine parseable logs.**
May 2-4, 2000	**Phrack56.tar.gz**	**Shared Library Redirection via ELF PLT Infection, Bypassing StackGuard and StackShield, Distributed portscanning tool DPS and script, and Cisco rerouting technique and tunneling script.**
May 2-4, 2000	Coopersniff01.zip	NT Sniffer includes a packet driver that sniffs packets from networks and displays full information for: Ethernet, IP, TCP, and UDP.
May 2-4, 2000	**Exman.c**	**A new man exploit.**
May 2-4, 2000	Outp.c	Converts .s files to shell code.
May 2-4, 2000	**RFParalyze.txt**	**Source code, which exploits Windows 95/98 NULL vulnerability.**
May 2-4, 2000	Cart32scan.pl	Script used to scan for the Cart32 vulnerability.
May 2-4, 2000	Sf.tar.gz	A front-end to the Arptool which sniffs connections to a switched network.
May 2-4, 2000	Saint-2.0.2.beta2.tar.gz	Security assessment tool which is based on SATAN.
May 2-4, 2000	Sara-3.0.2.tar.gz	Security Auditor's Research Assistant is a security analysis tool based on the SATAN model.
May 3, 2 000	**Gnobelib.c**	**Script which exploits the Gnomelib vulnerability in SuSE Linux 6.3.**
May 3, 2000	**UltraBoard.pl**	**Script which exploits the UltraBoard directory traversal vulnerability.**
May 3, 2000	**UltraBoard.cgi**	**Exploit for the UltraBoard directory traversal vulnerability.**
May 2, 2000	**Dnsloop.c**	**Exploit script for the Tcpdump 3.4-3.5 DNS loop vulnerability.**
May 2, 2000	**Lp-solaris7-of-x8c.c**	**Exploit script for the Solaris 7 LP vulnerability.**
May 2, 2000	**Sniffit.c**	**Exploit script for the Sniffit remote buffer overflow vulnerability.**
April 28 – May 1, 2000	Tcpb.c	A backdoor over non-connected and spoofed TCP packets.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
April 28 – May 1, 2000	Syslogd-DoS.c	Source code, which can be used to toy with a system's syslogd.
April 28 – May 1, 2000	RLRPAconv1.0.tar.gz	Remote Password Assasin is a network password cracker using brute force attacks.
April 28 – May 1, 2000	Nmap-2.51.tgz	Utility for network exploration or security auditing which fixes a target parsing vulnerability.
April 28 – May 1, 2000	**Mstream.c**	**Distributed Denial of Service (DDoS) source code.**
April 28 – May 1, 2000	Sftp02b.c	Smart FTP v0.2 Denial of Service exploit.
April 28 – May 1, 2000	Nmap02.50.tgz	Utility for network exploration, which supports ping scanning, many port scanning techniques, and TCP/IP fingerprinting.
April 26-27, 2000	Lpset.sh	Exploit for the Solaris/SPARC 2.7 lpset vulnerability.
April 26-27, 2000	4man.c	RedHat 6.1 /usr/bin/man exploit.
April 26-27, 2000	**Xsun2.c**	**Solaris 7 x86 local root stack overflow exploit.**
April 26-27, 2000	Sparc_lpset.c	Local root exploit for the SPARC lpset vulnerability.
April 26-27, 2000	Imwheel_ex.c	Imwheel local root exploit script.
April 26-27, 2000	Rp2.sh	Timbuktu Pro 2.0b650 Denial of Service exploit.
April 26-27, 2000	Xdnewsweb.pl	Exploit script for the vulnerability found in cgi DNEWSWEB.
April 26-27, 2000	Saint-2.0.2.beta1.tar.gz	Security assessment tool based on SATAN.
April 24-25, 2000	Ircii-dcc.tgz	Set of Perl scripts which exploits a Denial of Service vulnerability in ircii 4.4.
April 24-25, 2000	Sara-3.0.1.tar.gz	Security analysis tool based on the SATAN model.
April 24-25, 2000	Grout.tar.gz	Geographical tracerouter for Unix which combined the fastest tracerouter with the ability to display the location of intermediate machines.
April 24-25, 2000	Dig.c	Local buffer overflow exploit for x86 Linux.
April 24-25, 2000	Solx86-imapd.c	Remote root exploit for Solaris x86.
April 24-25, 2000	Solx86-nisd.c	Rpc.nisd remote root overflow exploit for Solaris 2.4 x86.
April 24-25, 2000	Lpset.c	Local root stack overflow exploit for the Solaris X86 lpset vulnerability.
April 24-25, 2000	Xsun.c	Solaris 7 x86 local root stack overflow exploit.
April 24-25, 2000	BISSE.zip	Broadcast Internet String Search Engine is a Windows-based scanner, which searches your network for services who have banners, matching a user-specified string.
April 24-25, 2000	Crazy.c	Unix based scanner, which scans for NT web vulnerabilities. Checks for 30 Cold Fusion files, IIS/IISadmin scripts, MSADC, and many other URLs that indicate a remote vulnerability.
April 24-25, 2000	Mio-star.tgz	Distributed multihosted Unix password cracker that runs on all platforms where Perl is installed.
April 24-25, 2000	Gnit_rcl.zip	GNIT Vulnerability Scanning Engine is for Win2K and NT systems which performs a port scan, and based on those findings, calls other functions.
April 24-25, 2000	Freebsd.mtr.c	Local root exploit script for the FreeBSD mtr vulnerability.
April 24-25, 2000	Nmap-2.30BETA21.tgz	Utility for network exploration, which supports ping scanning, many port scanning techniques, and TCP/IP fingerprinting.
April 24, 2000	Mmdump.pl	Exploit script for the Meeting Maker vulnerability.
April 21-23, 2000	**Lcdproc-exploit.c**	**Remote buffer overflow exploit script for the LCDProc vulnerability.**
April 21-23, 2000	Austinethack.tgz	Information on the Austnet hack and a slightly crippled demonstration code.
April 21-23, 2000	Wmaker.c	Exploit script for WindowMaker 0.62.0 buffer overflow vulnerability.
April 21-23, 2000	Kill_nwtcp.c	Buffer overflow script for the Novell Netware 5.1 vulnerability.
April 21-23, 2000	Panda-sec.zip	Demonstration exploit code for the Panda Security 3.0 vulnerability.
April 21-23, 2000	Regback.asm	Backdoor for NT written in pure ASM.
April 21-23, 2000	Ypghost050.tar.gz	Remote NIS exploit that spoofs UDP packets.
April 21-23, 2000	Sunkill.c	Remote Solaris 2.5.1 DoS exploit.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
April 21-23, 2000	Hupux.sh	HP-UX 09.04 local exploit which takes advantage of the default world writable /usr/local/bin.
April 21-23, 2000	Whois_raw.c	The whois_raw.cgi Perl script included in all freeware versions of the C domain package allows remote malicious users to view/retrieve any system files and to execute commands.

Script Analysis

When available, this section will supply a short description of scripts that have been analyzed by various security professionals and organizations. **We encourage you or your organization to contribute.** If you wish to do so, please send e-mail to nipc@fbi.gov with the subject line "CyberNotes Script Analysis." While space constraints may limit the length of descriptions in this document, contributors are requested to include a full technical analysis of the script along with release instructions. The release categories are: releasable to anyone; limited releasability (originator-defined list of organizations); or provided for NIPC only. A member of the CyberNotes editorial team will contact you. All contributions will be credited to the contributing individual or organization unless otherwise requested.

Trends

DDoS/DoS:

- **Reports of a combination of tools called "Mstream". The purpose of the tool is to enable intruders to utilize multiple Internet connected systems to launch packet-flooding Denial of Service attacks against one or more target systems.**
- **Phrack 56 published a script for a distributed portscanning tool named DPS. Both client and agent code are in the article "Distributed Tools".**
- An increasing number of reports of intruders using nameservers to execute packet-flooding Denial of Service attacks.

Probes/Scans:

- An increase in DNS scans from 211.53.208.178 from Korea, Portugal, Taiwan and Brazil.
- **A how-to has been published on the AMDROCKS BIND exploit.**
- **An increase from Brazil in exploits and scans to port 53, which are being used against two well-known vulnerabilities: NXT overflow vulnerability, which creates the directory ADMROCKS after entry; and the BIND vulnerability.**
- There has been an increase in probes to UDP Port 137 (NetBIOS Name Service).
- An increase in probes to port 1080/tcp (RingZero Trojan) and port 1243 (SubSeven Trojan).
- There has been an increase in port scans from Argentina and an increase in scans from Korean hosts that are aimed at port 111, 2974, and 4333. There has also been are reported increase in probes on ports 1080, 1953, and 31337. An increase in probes to ports 109/tcp, 137/udp, 138/udp, and 139/tcp has also been reported.

Other:

- **Hackers are rewriting the malicious "I Love You" virus that is circulating the globe. Antivirus firms identified at least eleven variations, including the original. Alterations in these variants are for the most part in the packaging, with the virus coming attached to e-mails variously labeled "I Love You," "FWD: JOKE," "Susitikim shi vakara kavos poudukul. . ." (Lithuanian for "Lets get a cup of coffee"), and "Mother's Day Order Confirmation."**
- **Continuing compromises of systems running various vulnerable versions of BIND (including machines where the system administrator does not realize a DNS server is running.**
- **There has been an increase in the recent distribution of worm variants of Melissa and PrettyPark.**
- An increase in reports of intruders exploiting unprotected Windows networking shares.
- Exploits are still being used against well-known vulnerabilities, the RDS DataFactory object and Microsoft IIS web servers, which is a component of Microsoft Data Access Components (MDAC).
- Reports indicate registry objects being maliciously altered which include: point of contact information for domain names, IP address delegations, and autonomous system numbers.

Viruses

W32/Santa.1104 (Win32.Santana) (Windows 32 Executable File Virus): On the Windows NT operating system W32/Santa.1104 is a non-resident file virus. However, on Windows 95/98 systems, it does become memory-resident, hooking the 'Change directory' system call.

This virus contains the following text, which never gets displayed:

Virus "SANTANA" created by Net'$ Wa$te [RespawneD EViL]

A file infected by the virus has reportedly been distributed as a cure for the W95/CIH-10xx virus via the Internet.

W95/Smash.10262 (Win95.Smash) (Windows 95 Executable File Virus): On the 14th of any month from June onwards, this virus will patch the IO.SYS system file so that on the next restart the hard disk will be overwritten with garbage.

It then displays a blue-screen error message and hangs the machine. The message says:

Virus Warning!
Virus name is 'SMASH', project D version 0x0A.
Created and compiled by Domitor.
Seems like your bad dream comes true...

WM97/Bablas-S (Word 97 Macro Virus): This virus has been reported in the wild. The virus resides in a module whose name is a euphemism for sexual intercourse.

The virus displays a message on the Word status bar telling the user to remove modules, which are not part of the virus:

Kill <Module> Macro in <Document>

where <Module> is the name of the module, and <Document> is the name of the currently active document.

WM97/Class-EQ (Word 97 Macro Virus): This virus has been reported in the wild and is a variant of the WM97/Class macro virus.

On the 30th of December, the virus displays the message box:

"lA-cOsA tE eSPiA!".

WM97/Claud-A (Word 97 Macro Virus): This virus has been reported in the wild and contains the following text as comments:

Este es un V macro, Elaborado por c l a u d I o
Este es el Comienzo de la era de los V Claudio

WM97/Coldape-V (Word 97 Macro Virus): This virus has been reported in the wild and is a variant of WM97/Coldape-A, which drops and attempts to run a malicious Visual Basic script.

If Windows Scripting Host is present, the script attempts to use Outlook Express to send an e-mail to a former editor of Virus Bulletin through an anonymous remailer.

The text of the message is "Dear Nicky ... my name is <Outlook username> and I want to make hot monkey love with you. You anti-virus stud!".

The script is detected as VBS/Coldape-Fam.

W97M/Marker.P (Word 97 Macro Virus): When a document is closed, the virus checks to see whether the template is already infected. W97M/Marker.P disables the macro protection system shipped with Word and prevents users from

confirming whether they want to save the changes made to the template. On February 22nd the virus deletes all the files found in the folder containing the infected document and displays an on-screen message.

WM97/Michael-C (Word 97 Macro Virus): This virus has been reported in the wild and is very similar to WM97/Michael-B.

The virus uses the Office Assistant to display a random message, chosen from 21 possibilities.

These include messages credited to Dr Who, Einstein, Dorothy Parker, Virginia Woolf, Steve McConnell, David Parnas and Paul Clements, Kreitzberg and Schneiderman, Alice in Wonderland, Michael I. Buen, Glenford Myers, Donald Knuth, Peter Williams and Rich Cook.

If it is a Friday and the day of the month is after the 23rd, the virus will attempt to intercept the FilePrint command and print another document instead. This claims to be virus author's resume.

At the end of the printout is the following message:

> Warning: If I don't get a stable job by the end of the month I
> will release a third virus that will remove all folders in the
> Primary Hard Disk, or in layman's term para ko na ring fi-normat
> ang Hard Disk Mo

WM97/Myna-N (Word 97 Macro Virus): This virus has been reported in the wild and contains no intentionally malicious code. The replicating code contains the phrase MYNAMEISVIRUS, which is used as a flag to check for its presence.

W97M/Laroux.CA (Excel 97 Macro Virus): The virus creates a file called PERSON2.XLS in the Microsoft Excel 97 start folder, through which it carries out infections. These are produced when Excel is run, upon which PERSON2.XLS is automatically opened.

W97M/Talon.M (Word 97 Macro Virus): Every Sunday, W97M/Talon.M displays a message similar in style to those used by the Office Assistant. In addition, this virus triggers a payload in August that consists of deleting two of the system files used to boot a computer: the command interpreter, COMMAND.COM, and the hidden file IOSYS.SYS. This makes it impossible to start up the infected machine.

XM97/Laroux-MP (Excel 97 Macro Virus): This virus has been reported in the wild and is another variant of XM/Laroux, which contains two macros, AUTO_OPEN and CHECK_FILES.

The AUTO_OPEN macro is run when the infected document is opened, and instructs Excel to call the CHECK_FILES macro every time a new worksheet is activated.

When this happens, the virus creates a file in the XLSTART directory called PERSONAL.XLS and copies the viral macros into it. This file is automatically opened every time Excel is run. From then on it infects every workbook used. When PERSONAL.XLS is infected, the virus will be loaded every time Excel is started.

XM97/Vcx-J (Excel 97 Macro Virus): This virus has been reported in the wild. It is an Excel macro virus, which writes an infected file called XLSCAN.XLS to the Excel Startup folder when an infected spreadsheet is closed.

The virus also writes files to the Windows System folder called xxxxxx.vcx where xxxxxx is the numerical value of the month, day, hour, minute and second.

VBS/LoveLetter-A (Visual Basic Script Worm): This virus has been very widely reported in the wild. It is a virus, which tries to spread itself in several ways. Most commonly, it sends itself as an attachment to an e-mail.

Infected emails have the subject line:

> ILOVEYOU

The message text is:

kindly check the attached LOVELETTER coming from me.

The attachment is called "LOVE-LETTER-FOR-YOU.TXT.vbs", which has a "double extension". Mailers, which suppress well-known extensions such as .vbs, may present this file as "LOVE-LETTER-FOR-YOU.TXT", which appears more innocent.

Because the virus arrives in a VBS file, it requires the Windows Scripting Host (WSH) in order to work. If you disable WSH, the viral attachment will be rendered harmless.

The virus also drops an HTM file, which can spread the virus, and a mIRC script, which tries to distribute it. It also tries to download a file called WIN-BUGSFIX.exe from the internet, and injects two copies of its VBS script into the system directory where they are executed each time the computer reboots.

The e-mail component of the virus requires Microsoft Outlook to work. If you are using Outlook it will try to send itself to each entry in your Windows Address Book.

Antivirus firms identified at least eleven variations, including the original. Alterations in these variants are for the most part in the packaging, with the virus coming attached to e-mails variously labeled "I Love You," "FWD: JOKE," "Susitikim shi vakara kavos poudukul. . ." (Lithuanian for "Lets get a cup of coffee"), and "Mother's Day Order Confirmation."

The following table lists "The Love Bug" and six of its variants spotted so far.

Subject	Attachment Name	Seen "in the wild"
I Love You	LOVE-LETTER-FOR-YOU-TXT.vbs	Yes
Susitikim shi vakara kavos poudukul…	LOVE-LETTER-FOR-YOU-TXT.vbs	Yes
FWD: JOKE	VERYFUNNY.vbs	Yes
I Love You	LOVE-LETTER-FOR-YOU-TXT.vbs	Yes
Mother's Day Order Confirmation	Mothersday.vbs	No
Dangerous Virus Warning	Virus_warning.jpg.vbs	Yes
VIRUS ALERT!!!	Protect.vbs	Yes
A killer for VBS/LoveMail and VBS/Kak worm	Viruskiller.vbs	Yes

Jane.B (Worm): This worm spreads through mIRC as Jane.BMP.EXE, designed to compromise security on infected machines. Because of the unique file name, many users believe they are receiving an image file instead of an executable.

JS/Unicle-A (W32/RUNFTP.WORM.SCRIPT) (JavaScript Virus): This virus has been reported in the wild and is a JavaScript virus. It only functions fully on Chinese versions of Windows 95/98 which have Internet Explorer 5 and the Windows Scripting Host installed and use Outlook or Outlook Express as an email reader. Support for JavaScript must also be enabled.

The virus exploits security holes in the implementation of 'Scriptlet.typelib' in ActiveX. Microsoft has released a patch, which fixes these security holes. For further information and to download the patch please view Microsoft Security Bulletin (MS99-032).

When an infected e-mail message is opened the virus creates the file 'Microsoft Internet Explorer.hta' in the Windows Startup folder. When 'Microsoft Internet Explorer.hta' is run it creates a file 'Msie.hta' in the System folder, modifies 'Win.ini' to run 'Msie.hta' when Windows is started and runs 'Msie.hta'. 'Msie.hta' attempts to download and run a file from one of ten FTP sites and deletes 'Microsoft Internet Explorer.hta'.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. The increasing number of Trojans gains added significance due to recent testing conducted to determine the ability of anti-virus software to detect Trojans. According to the test results, a number of popular anti-virus products failed to detect or had limited detection capabilities against current popular Trojans. Testing also indicates that detection of a baseline Trojan does not necessarily mean the anti-virus software can detect a variant. Readers should contact their anti-virus vendors to obtain specific information on Trojans and their variants that their software detects.

The following table provides the reader with a list of Trojans that have received write-ups in this publication. This table starts with Trojans discussed in CyberNotes #2000-01 and will be added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks.

Trojan	Version	Issue discussed
Acid Shiver + lmacid	v1.0 + 1.0Mod	CyberNotes-2000-07
AOL Trojan		CyberNotes-2000-01
BioNet	**v0.84 - 0.92**	**Current Issue**
Bla	1.0-5.02	CyberNotes-2000-06
Bla	**v1.0 - 5.03**	**Current Issue**
Bobo	**v1.0 - 2.0**	**Current Issue**
DeepThroat	v1.0 - 3.1 + Mod (Foreplay)	CyberNotes-2000-05
Delta Source	J0.5b-0.7	CyberNotes-2000-01
Donald Dick	1.52-1.55	CyberNotes-2000-01
Drat	**v1.0 - 3.0b**	**Current Issue**
FakeFTP	Beta	CyberNotes-2000-02
Girlfriend	V1.3x (including Patch 1 & 2)	CyberNotes-2000-05
Hack`a`Tack	1.2-2000	CyberNotes-2000-06
Hack'A'tack	1.0-2000	CyberNotes-2000-01
ik97	v1.2	CyberNotes-2000-07
InCommand	1.0-1.4	CyberNotes-2000-01
InCommand	**v1.0 - 1.5**	**Current Issue**
Infector	**v1.0 - 1.42**	**Current Issue**
Infector	v1.3	CyberNotes-2000-07
iniKiller	**v1.2 - 3.2**	**Current Issue**
Intruder		CyberNotes-2000-01
Kuang Original	0.34	CyberNotes-2000-01
Matrix	1.4-2.0	CyberNotes-2000-01
Matrix	**v1.0 - 2.0**	**Current Issue**
MoSucker		CyberNotes-2000-06
Naebi	**v2.12 - 2.39**	**Current Issue**
NetController	v1.08	CyberNotes-2000-07
NetSphere	**v1.0 - 1.31337**	**Current Issue**
NetSphere	v1.0 - 1.31337	CyberNotes-2000-06
NetTrojan	1.0	CyberNotes-2000-06
Nirvana / VisualKiller	v1.94 - 1.95	CyberNotes-2000-07
Phaze Zero	**v1.0b + 1.1**	**Current Issue**
Prayer	1.2-1.3	CyberNotes-2000-06
Prayer	**v1.2 - 1.5**	**Current Issue**
Prosiak	**beta - 0.65**	**Current Issue**
Setup Trojan (Sshare) +Mod Small Share		CyberNotes-2000-06

Trojan	Version	Issue discussed
ShadowPhyre	v2.12.38 - 2.X	CyberNotes-2000-06
ShitHeap		**Current Issue**
Softwarst		CyberNotes-2000-05
SubSeven	1.0-2.1c	CyberNotes-2000-01
SubSeven	1.0-2.1Gold	CyberNotes-2000-02
SubSeven	V1.0-1.9b, v2.1+SubStealth, v2.2b1	CyberNotes-2000-07
Trinoo		CyberNotes-2000-05
TryIt		CyberNotes-2000-05
wCrat	v1.2b	CyberNotes-2000-05

BioNet v0.84 - 0.92 (April 29, 2000): The 0.8x versions of this Trojan are Windows 95/98 only. However the 0.9x (and above) have versions each for 95/98 And NT. The client-server protocol is the same, so an NT client can hack a 95/98 infected machine, and a 95/98 client can hack an NT infected system just the same.

File transfer, message boxes, screen and key capture, move mouse and reboot/shutdown are a few of its commands.

You usually notice you're infected because you no longer can reboot or shutdown the computer (as the Trojan wont shutdown.) It also makes it impossible to reboot to MSDOS mode to delete the Trojan.

Bla v1.0 - 5.03 (April 26, 2000): This Trojan only seems to have basic file upload and download commands, as well as message box features. It can also send all of your system passwords back to the hacker, as well as let them lockup or reboot your computer. Version 2.0 has new features that allow it to grab your passwords and lockup your system.

Bobo v1.0 - 2.0 (April 29, 2000): Another Trojan, basically a small subset of commands from BackOrifice, with much the same interface as the BackOrifice GUI. This Trojan has no registry editor commands or plugin support.

Drat v1.0 - 3.0b (April 26, 2000): Drat is a rather resourceful Trojan in many ways. First noticeable difference, there is no client software for hackers to use. They can simply telnet to your computer (telnet being software almost all computers come with) and do their damage that way. With the aid of a small helper program, one can even transfer files to and from you. This basically gives hackers 'dos' like access to your computer, however with even more commands.

The other noticeable thing is the way it loads itself. Drat will replace a section of Windows, so that any time you run a .exe or .bat file, drat reloads! Drat will also reload when the computer is shutting down. This means you can't run regedit to remove drat, without also reloading drat on your system.

Furthurmore, if you simply delete the file, thinking Drat was the .exe and .bat handler, windows will not be able to run any .exe files again. The only way to fix what Windows uses to load .exe's is to use regedit. However, regedit is an .exe, thus you will not be able to run it in Windows.

Hack`a`Tack 1.0 - 2000 (April 29, 2000): This Trojan is mostly a file transfer server that scans for other Trojans using an infected host, and can get basic information about your computer. Its main usefulness is to install other more featured Trojans onto your system.

v2000 (hat2k) is Shareware. The client a hacker would use is very limited unless they pay for it first. No major updates (other than the shareware change) are stated in the Readme.

InCommand v1.0 - 1.5 (April 29, 2000): This Trojan seems to have the standard file transfer, program control, and registry editing ability, but does have potential to be damaging.

Infector v1.0 - 1.42 (April 29, 2000): Infector does not let others control your computer. All this Trojan does is send an ICQ to a specified person, giving them your IP when you are online.

This would be used mostly when you are infected with a different type of Trojan that doesn't have ICQ notify built in.

iniKiller v1.2 - 3.2 Pro (April 27, 2000): This is a basic Trojan with a few destructive commands which can easily destroy data on your system.

Matrix v1.0 - 2.0 (April 29, 2000): This is a Trojan based on the sourcecode to Girlfriend Trojan. Its main features seems to be an FTP like file server, and the ability to update the Trojan exe on a victims computer to a newer version with one button click.

Naebi v2.12 - 2.39 (April 26, 2000): The documents with this Trojan are not in English; however, its main function is a password logger, and it has basic file manipulation commands. This Trojan attaches to the ICQ preferences in your registry, running when ICQ would. New in version 2.34 and above, the Trojan can obtain passwords from most common ftp programs, dialup networking, all system password file lists, ICQ, as well as other Trojans if you happen to be infected, such as Netbus, and Backorifice.

NetSphere v1.0 - 1.31337 (April 27, 2000): This Trojan has all the features you see in NetBus, plus a few extra such as: Kill CPU, add to ICQ, see the open ports on target, IP scan, view ALL hidden windows processes, etc.

Phaze Zero v1.0b + 1.1 (April 29, 2000): Phaze Zero has basic netbus like features, just like most of the others. This Trojan listens on TCP port 555, and like netbus is easily removed.

Prayer v1.2 - 1.5 (April 29, 2000): This Trojan is not in English; however, apparently there are quite a number of features the client supports. This Trojan can perform file transfers, run programs, restart the computer, etc. It seems to mirror the standard/common features of NetBus.

Prosiak beta - 0.65 (April 29th, 2000): This Trojan has the standard features, and for the most part can only manipulate your files and run programs.

ShitHeap (April 28, 1999): Another basic Trojan, trying to hide as your recycle bin this time.